In the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Please amend the claims as follows:

1. (Currently Amended) A smartcard transaction system configured with a biometric security device, said system comprising:

a smartcard configured to communicate with a reader wherein said reader and said biometric security device are configured to communicate with a host;

said biometric security device comprises a fingerprint sensor to detect a proffered fingerprint sample, said fingerprint sensor configured to communicate with said host;

a verification device configured to compare said proffered fingerprint sample with a registered fingerprint sample, wherein said registered fingerprint sample is primarily associated with a preset transaction limitation ~~first user account~~ and secondarily associated with a ~~second~~ user account, and wherein said verification device is further configured to verify whether said proffered biometric sample is associated with said preset transaction limitation and to verify compliance with said preset transaction limitation~~, and wherein said second user account is different than said first user account~~; and

wherein said smartcard is configured to utilize ~~at least one of~~ said ~~first~~ user account ~~and said second user account~~ to facilitate a smartcard payment transaction.

2. (Previously Presented) The smartcard transaction system of claim 1, wherein said biometric security device is configured to communicate with said host via at least one of said smartcard, said reader, and a network.

3. (Original) The smartcard transaction system of claim 1, wherein said fingerprint sensor is configured to facilitate a finite number of scans.

4. (Previously Presented) The smartcard transaction system of claim 1, wherein said fingerprint sensor is configured to store log data comprising at least one of a detected fingerprint

sample, processed fingerprint sample and registered fingerprint sample, and wherein said fingerprint sensor is further configured to employ a security procedure when said proffered fingerprint sample differs from said log data.

5. (Original) The smartcard transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered fingerprint samples, proffered and registered user information, terrorist information, and criminal information.

6. (Previously Presented) The smartcard transaction system of claim 5, wherein said database is contained in at least one of said smartcard, said reader, said fingerprint sensor, a remote server, a merchant server and said smartcard transaction system.

7. (Previously Presented) The smartcard transaction system of claim 6, wherein said database is configured to be operated by an authorized sample receiver.

8. (Previously Presented) The smartcard transaction system of claim 1, wherein said fingerprint sensor is configured with at least one of an optical scanner and capacitance scanner.

9. (Previously Presented) The smartcard transaction system of claim 1, wherein said fingerprint sensor is configured to detect and verify finger print minutia including at least one of ridge endings, bifurcation, lakes, enclosures, short ridges, dots, spurs, crossovers, pore size, pore location, loops, whorls, and arches.

10. (Previously Presented) The smartcard transaction system of claim 1, wherein said fingerprint sensor is configured to include an additional sensor to detect and verify at least one of blood flow, correctly aligned ridges, pupil dilation, pressure, motion, and body heat.

11. (Cancelled)

12. (Currently Amended) The smartcard transaction system of claim 1, wherein said registered fingerprint sample is stored by at least one of a third-party biometric security vendor and a governmental agency ~~verification device is at least one of a third party security vendor device and a local CPU~~.

13. (Cancelled)

14. (Cancelled)

15. (Previously Presented) The smartcard transaction system of claim 1, wherein different registered fingerprint samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

16. (Currently Amended) The smartcard transaction system of claim 1, wherein said ~~first~~ user account comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information~~, and wherein said second user account comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information~~.

17. (Original) The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered fingerprint sample.

18. (Original) The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered fingerprint sample.

19. (Previously Presented) The smartcard transaction system of claim 1, wherein said fingerprint sensor is configured to provide a notification upon detection of a sample, and wherein said notification is at least one of a notification to a security vendor, a notification to a store

employee, and a notification to a primary account holder that said primary account is being accessed.

20. (Previously Presented) The smartcard transaction system of claim 1, wherein said verification device is further configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

21. (Previously Presented) The smartcard transaction system of claim 1, wherein said verification device is configured to facilitate the use of a secondary security procedure which includes sending a signal to said host to notify that a condition of use for said smartcard is being violated.

22. (Currently Amended) A method for facilitating biometric security in a smartcard transaction system comprising:

registering a fingerprint sample by primarily associating said fingerprint sample with a preset transaction limitation ~~first user account~~ and secondarily associating said fingerprint sample with a ~~second~~ user account to create a registered fingerprint sample~~, wherein said second user account is different than said first user account~~;

proffering a fingerprint to a fingerprint sensor communicating with said system to form a proffered fingerprint sample; and

using ~~selecting at least one of said first user account and~~ said ~~second~~ user account to facilitate a smartcard payment transaction upon verification of said proffered fingerprint sample against said registered fingerprint sample, wherein said verification includes verification of compliance with said preset transaction limitation.

23. (Previously Presented) The method of claim 22, wherein said step of registering comprises contacting an authorized sample receiver.

24. (Previously Presented) The method of claim 23, wherein said step of registering further includes at least one of: proffering said fingerprint to said authorized sample receiver,

processing said fingerprint to obtain said fingerprint sample, verifying said fingerprint sample, and storing said fingerprint sample upon verification.

25. (Previously Presented) The method of claim 22, wherein said step of proffering includes proffering said fingerprint to at least one of an optical scanner and a capacitance scanner.

26. (Previously Presented) The method of claim 22, wherein said step of proffering further includes proffering said fingerprint to said fingerprint sensor communicating with said system to initiate at least one of: storing, comparing, and verifying said fingerprint sample.

27. (Previously Presented) The method of claim 22, wherein said step of proffering further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

28. (Cancelled)

29. (Previously Presented) The method of claim 22, wherein said step of verifying includes comparing said proffered fingerprint sample to said registered fingerprint sample, wherein said registered fingerprint sample is registered with at least one of a third-party biometric security vendor and a governmental agency ~~by using at least one of a third party security vendor device and a local CPU~~.

30. (Previously Presented) The method of claim 22, wherein said step of verifying includes comparing fingerprint minutia.

31. (Previously Presented) The method of claim 30, wherein said step of comparing fingerprint minutia comprises storing, processing and comparing at least one of ridge endings, bifurcation, lakes, enclosures, short ridges, dots, spurs, crossovers, pore size, pore location, loops, whorls, and arches.

32. (Previously Presented) The method of claim 22, wherein said step of proffering further comprises using said fingerprint sensor to detect at least one of blood flow, correctly aligned ridges, pupil dilation, pressure, motion, and body heat.

33. (Previously Presented) The method of claim 22, wherein said step of proffering further includes at least one of detecting, processing and storing a second proffered fingerprint sample.

34. (Previously Presented) The method of claim 22, wherein said step of proffering further includes the use a secondary security procedure which includes sending a signal to a host to notify that a condition of use for a smartcard is being violated.

35. (Currently Amended) A method for facilitating biometric security in a smartcard transaction system comprising:

receiving data from a smartcard via a reader which communicates with said system;

detecting a proffered fingerprint at a sensor which communicates with said system to obtain a proffered fingerprint sample;

verifying said proffered fingerprint sample by comparing said proffered fingerprint sample with a registered fingerprint sample, wherein said registered fingerprint sample is primarily associated with a preset transaction limitation ~~first user account~~ and secondarily associated with a ~~second~~ user account~~, and wherein said second user account is different than said first user~~;

using ~~at least one of said first user account and~~ said ~~second~~ user account to facilitate a smartcard payment transaction; and,

authorizing said smartcard payment transaction to proceed upon verification of said proffered fingerprint sample, said verification including determining compliance with said preset transaction limitation.

36. (Previously Presented) The method of claim 35, wherein said step of detecting further includes detecting said proffered fingerprint at said sensor which communicates with said system via at least one of said smartcard, said reader, and a network.

37. (Previously Presented) The method of claim 35, wherein said step of detecting ~~said~~ proffered fingerprint includes detecting said proffered fingerprint by at least one of a capacitance scanner and an optical scanner.

38. (Previously Presented) The method of claim 35, wherein said step of detecting includes at least one of: detecting, storing, and processing said proffered fingerprint sample.

39. (Previously Presented) The method of claim 35, wherein said step of detecting further includes receiving a finite number of proffered fingerprint samples.

40. (Previously Presented) The method of claim 35, wherein said step of detecting further includes storing log data information comprising at least one of a detected fingerprint sample, a processed fingerprint sample and said registered fingerprint sample, and wherein said fingerprint sensor is further configured to employ a security procedure when said proffered fingerprint sample differs from said log data information.

41. (Previously Presented) The method of claim 35, wherein said step of detecting further includes at least one of detecting, processing and storing a second proffered fingerprint sample.

42. (Original) The method of claim 35, wherein said step of detecting further includes using said fingerprint sensor to detect at least one of blood flow, correctly aligned ridges, pupil dilation, pressure, motion, and body heat.

43. (Cancelled)

44. (Previously Presented) The method of claim 35, wherein said step of comparing said proffered fingerprint sample with said registered fingerprint sample comprises storing, processing and comparing fingerprint minutia.

45. (Previously Presented) The method of claim 35, wherein said step of comparing said proffered fingerprint sample with said registered fingerprint sample includes comparing said proffered fingerprint sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

46. (Previously Presented) The method of claim 35, wherein said step of verifying includes verifying said proffered fingerprint sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

47. (Currently Amended) The method of claim 35, wherein said step of verifying includes verifying said proffered fingerprint sample by comparison to a registered fingerprint sample registered with at least one of a third-party biometric security vendor and a governmental agency ~~using at least one of a local CPU and a third-party security vendor~~.

48. (Previously Presented) The smartcard transaction system of claim 1, wherein said proffered fingerprint sample is further configured as at least one of a variable in an encryption calculation to secure data, and as both a private key and a public key for encryption purposes.

49. (Previously Presented) The method of claim 22, further comprising using said proffered fingerprint sample as at least one of a variable in an encryption calculation for securing data, and as both a private key and a public key for encryption purposes.

50. (New) The system of claim 1, wherein said preset transaction limitation comprises at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.

51. (New) The method of claim 22, wherein said preset transaction limitation comprises at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.

52. (New) The method of claim 35, wherein said preset transaction limitation comprises at least one of a maximum transaction amount, minimum transaction amount, maximum number of transactions within a time period, maximum number of transactions, use by certain merchants, temporal limitation, geographic limitation, and use of non-monetary funds.